

**DOCKET NO.:** MSFT-2867/306926.02  
**Application No.:** 10/820,673  
**Office Action Dated:** May 1, 2006

**PATENT**

**Amendments to the Drawings**

The attached sheet of drawings includes changes to Fig 1. The sheet(s), which includes Fig(s) 1, replaces the original sheet(s) including Fig(s) 1.

Attachment: Replacement Sheet(s)

**REMARKS**

The foregoing Amendment and the following Remarks are submitted in response to the Office Action issued on May 1, 2006 in connection with the above-identified patent application, and are being filed within the three-month shortened statutory period set for a response by the Office Action.

Claims 1-23 remain pending in the present application as amended. Claims 1, 7, 12 and 23 have been amended. Applicants respectfully submit that no new matter has been added to the application by the Amendment.

Applicants respectfully request reconsideration and withdrawal of the rejection of the claims, consistent with the following remarks.

The Examiner notes that Fig. 1 of the present application should bear a - - Prior Art - - legend, and has required corrected drawings. Accordingly, attached is a drawing sheet with corrected Fig. 1 having such legend.

The Examiner has provisionally rejected claims 1-23 under the judicially created doctrine of obviousness-type double patenting in view of claims 1-16 of co-pending US Patent Application No. 10/820,666. Applicants respectfully traverse the double patenting rejection insofar as the conflicting claims have not issued in a US patent. Applicants will timely file an appropriate terminal disclaimer to obviate any double patenting rejection if and when such double patenting rejection becomes definite.

The Examiner has rejected claim 7 under 35 USC § 112, second paragraph for the reason that such claim 7 includes a stray reference numeral. Accordingly, Applicants have amended such claim 7 to remove the reference numeral, and thus request reconsideration and withdrawal of the § 112, second paragraph rejection.

The Examiner has rejected claims 1-23 under 35 USC § 103 as being obvious over Olik (U.S. Patent Application No. 2002/0023207) in view of Stefik (U.S. Patent No. 5,715,403). Applicants respectfully traverse the § 103 rejection insofar as it may be applied to the claims as amended.

Independent claim 1 as amended recites a computing device such as a personal computer or the like that has instantiated thereon a protected media path for delivering content from at least one source to at least one sink. As was pointed out in the specification

of the present application, the source may be any of several highly functional or minimally functional rights management systems, or may be any of several sources with limited content protection. As was also pointed out, the source may obtain the actual content from elsewhere. For example, the content if rights-protected may be located on a remote file server but accessible by way of a source such as a rights management system on the computing device. Generally, then, a source is capable of sourcing multimedia data in a generic manner through a given interface.

Similarly, and as was also pointed out in the specification of the present application, the sink is a system receiving or 'sinking' the content and may be any appropriate system that can interact with the media base. For example, the sink may be an audio system for receiving audio to be delivered to a speaker, a video system for receiving video to be delivered to a display, a light control system for receiving light control signals to be delivered to a controller for a light system, a motor control system for receiving motor control signals to be delivered to a controller for a motor system, and the like. As with the source, the sink may deliver the actual content to elsewhere. For example, the content if audio may be delivered to a remote speaker by way of a sink such as a sound card on the computing device.

In the protected media path on the computing device, a media base provides a protected environment in the computing device and includes a common infrastructure of core components effectuating processing of content from any particular source and delivering the processed content to any particular sink, and also includes a policy engine enforcing policy on behalf of each source. As may be appreciated, the processing effectuated by the media base is in the nature of any processing that may be performed on content and especially decrypted content, including dividing out streams therefrom, filtering and aligning each stream, etc.

As set forth in claim 1, the policy corresponds to the content from the source and includes rules and requirements for accessing and rendering the content. Thus, the media base is trusted by the source to enforce any policy associated with the content. For example, if the content is rights-protected and according to the source should not be copied, the media base will effectuate prevention of such copying. Accordingly, the media base allows content to flow through the computing device in a protected fashion, and allows for arbitrary

processing of the protected content in the computing device, even if the content is decrypted while being processed in the computing device.

As recited in claim 1, a source trust authority (SOTA) is provided in the computing device in the protected media path, and is associated with and corresponds to the source of the content. Thus, the SOTA is separate from but represents the source within the protected media path. The SOTA in effect acts as a secure lockbox that connects the source to the media base and that represents the source in the protected media path. Also, the SOTA decrypts the content from the source, and translates policy associated with the content from a native format into a format amenable to the policy engine.

Likewise, a sink trust authority (SITA) is provided in the computing device in the protected media path, and is associated with and corresponds to the sink of the content. Thus, and again, the SITA is separate from but represents the sink within the protected media path, and in effect also acts as a secure lockbox connecting the sink to the media base and representing the sink in the protected media path. Here, the SITA encrypting content to be delivered to the sink, and translates the policy associated with the content from the format of the policy engine into a format amenable to the sink. Thus, the sink with the encrypted content and corresponding policy decrypts the content and renders same based on the received policy.

Independent claim 12 as amended recites a method with regard to the protected media path of claim 1. In particular, claim 12 recites that to deliver the content of claim 1 from the source to the sink, an application on the computing device calls to the media base with a definition of the content, the source, and the sink, and the media base establishes the protected media path based on the defined content, source, and sink to effectuate such delivery, where the established protected media path includes the media base, the SOTA, and the SITA.

Thereafter, the SOTA on behalf of the source establishes trust with respect to the protected media path, perhaps by way of collecting proffers of trust from the elements of the path. Upon trust being established with respect to the protected media path, the SOTA then propagates the policy corresponding to the content to be delivered to the protected media path. Such policy is typically propagated first to the media base and then to the SITA,

whereby the establishment of trust ensures the SOTA that the propagated policy will in fact be honored by each element.

The SOTA determines a particular type of action to be taken with the content as delivered through the protected media path, where the action may for example be to render the content, to copy the content, etc., the SOTA decides whether the particular type of action can in fact be taken with the content as delivered through the protected media path, and the SOTA then informs the media base regarding the decision. The media base informs the application whether the particular type of action can be taken, and if so the application proceeds by commanding the media base to perform such type of action.

The Olik reference discloses a system where data is securely passed between a client 10 (Fig. 1) at one computing device and a back-end resource 22 at another computing device 20 by utilizing an intermediary / proxy / enabler 24 that substitutes references for data and functions as if it were in fact a client. When sending service requests to a web-server 32 on a publicly-accessible site, the intermediary / enabler 24 replaces the data with references; when the enabler 24 receives references from the publicly-accessible site, such enabler 24 replaces those references with the actual data. Thus, and as best seen in Fig. 3, the intermediary / enabler 24 prevents the web-server 32 from having access to the data.

Preliminarily, Applicants respectfully point out that the processes and elements of the Olik reference are spread over multiple computing devices, and thus are not parts of a protected media path instantiated on a computing device, as is required by claims 1 and 12. Instead, the Olik path is established by the multiple computing devices being interconnected by way of network connections 14 and 16 (Fig. 1).

Moreover, the Olik reference only sets forth communications between computing devices, and does not include any trust authorities such as SITAs and SOTAs that represent such devices. In particular, the Olik reference does not disclose or even suggest that a protected media path is established to include a media base, a SOTA representative of a source of content, and a SITA representative of a sink or destination for such content, as is required by claims 1 and 12. To summarize thus far, then, the present invention as recited in claims 1 and 12 requires a source, a SOTA, a media base, a SITA, and a sink, while the Olik reference at most discloses a source (the client 10), a destination (back-end resource 22, and

not the web-server 32), and an intermediary / enabler 24 whose purpose is to ensure that the web-server 32 does not access transmitted data.

To continue, the Olik reference sets forth that the data from the client 10 is represented to the web-server 32 by way of a reference such that the web-server never actually has access to the data, but instead only has access to the reference. Thus, the web-server 32 commands the back-end resource 22 to perform an action with regard to the data by including the reference to the data. With regard to the present invention, then, the enabler 24 does not perform any actual processing on the data / content, as is required by claims 1 and 12, other than storage and the like.

Significantly, the Olik reference does not at all disclose or even consider that the data / content may have associated policy, and that the enabler 24 thus should or even could have a policy engine that enforces any such policy on behalf of the client 10, as is required by claims 1 and 12. In particular, the Olik data does not have policy that includes rules and requirements for accessing and rendering the content as is required by claims 1 and 12.

Further, the Olik reference does not disclose or even suggest that the data thereof may be encrypted, or that any SOTA representing the client 10 in effect acts as a secure lockbox that connects the client 10 to the enabler 24, that represents the client 10 in any protected media path, that decrypts the data from the client 10, and that translates policy associated with the data from a native format into a format amenable to any policy engine of the enabler 24, all as is required by claims 1 and 12. Similarly, the Olik reference does not disclose or even suggest that any SITA representing the back-end resource 22 in effect acts also acts as a secure lockbox connecting the sink to the media base, that represents the resource 22 in any protected media path, that encrypts content to be delivered to the resource 22, and that translates the policy associated with the content from the format of any policy engine into a format amenable to the resource 22, all as is required by claims 1 and 12. Likewise, the resource 22 is not set forth as decrypting the content and rendering same based on the received policy, as is required by claims 1 and 12.

Moreover, the Olik reference does not disclose or suggest that any SOTA acting on behalf of the client 10 establishes trust with respect to any protected media path, and thereafter propagates policy corresponding to content to be delivered to the protected

media path, as is required by claim 12. Likewise, the Olik reference wholly fails to disclose or even realize that the such a SOTA should or even could determine a particular type of action to be taken with the content as delivered through the protected media path, decide whether the particular type of action can in fact be taken with the content as delivered through the protected media path, and inform the enabler 24 regarding the decision, where such enabler 24 would then inform an application on the computing device whether the particular type of action can be taken, and if so the application proceeds by commanding the media base to perform such type of action, all as is required by claim 12.

The Examiner cites to the Stefik reference only for the purpose of disclosing the use of policy with regard to content. Accordingly, Applicants respectfully submit that the Stefik reference also wholly fails to disclose or even suggest the SOTA, media base, SITA, and protected media path of claims 1 and 12. Further, Applicants respectfully submit that the Stefik reference fails to disclose such a SOTA performing the particular method steps recited in claim 12 with regard to policy as applied to the aforementioned SOTA, media base, SITA, and protected media path of claim 12.

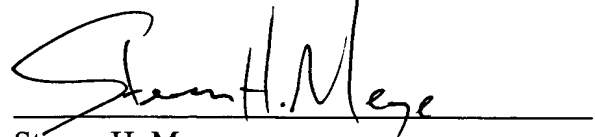
Accordingly, Applicants again respectfully submit that the Olik reference and Stefik reference cannot be applied to make obvious claims 1 or 12, or any claims depending therefrom. Accordingly, Applicants respectfully request reconsideration and withdrawal of the § 103 rejection.

**DOCKET NO.:** MSFT-2867/306926.02  
**Application No.:** 10/820,673  
**Office Action Dated:** May 1, 2006

**PATENT**

In view of the foregoing discussion, Applicants respectfully submit that the present application including claims 1-23 is in condition for allowance, and such action is respectfully requested.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Steven H. Meyer", is written over a horizontal line.

Steven H. Meyer  
Registration No. 37,189

Date: July 24, 2006

Woodcock Washburn LLP  
One Liberty Place - 46th Floor  
Philadelphia PA 19103  
Telephone: (215) 568-3100  
Facsimile: (215) 568-3439